U.S. House of Representatives

The Committee on Energy and Commerce

Subcommittee on Oversight and Investigations Hearing:

"Internet Data Brokers and Pretexting: Who has Access to Your Private Records?"

September 29, 2006

Testimony of Mr. Charles Wunsch

Summary of Major Points

1. **Sprint Nextel appreciates the opportunity to share its views on protection of customer information and the problem of pretexting.**
2. **Sprint Nextel views pretexting as a wrong that should be stopped.**
3. **Sprint Nextel takes protecting customer information seriously and has received an award for its efforts.**
4. **Protecting customer privacy must be done in the context of customer demands for reasonable access to their account information.**
5. **Sprint Nextel protects customer information by implementing system protections combined with privacy training for appropriate employees.**
6. **Sprint Nextel encourages its customers to take actions to protect their information, such as frequently changing passcodes.**
7. **Sprint Nextel constantly reviews its privacy protections with the view to improving them.**
8. **To that end, Sprint Nextel has actively and successfully confronted pretexters through litigation and cease and desist letters.**

U. S. House of Representatives

The Committee on Energy and Commerce

Subcommittee on Oversight and Investigations Hearing:

"Internet Data Brokers and Pretexting: Who has Access to Your Private Records?"

September 29, 2006

Testimony of Mr. Charles Wunsch

Chairman Whitfield, Ranking Member Stupak, thank you for the invitation to testify before the Subcommittee today. I appreciate this opportunity to represent the third largest carrier in the wireless industry, Sprint Nextel Corporation. I ask that my full written statement be entered into the record.

My name is Charles Wunsch, and I am the Vice President for Corporate Transactions and Business Law at Sprint Nextel. I oversee Sprint Nextel's Office of Privacy. We are proud of our privacy accomplishments at Sprint Nextel given the difficulties of balancing the interests of customer privacy and customers' desire for easy access to their account information.

Sprint Nextel devotes substantial resources to protecting the privacy of its customers' confidential information. Our Corporate Security, Legal and Customer Care teams regularly evaluate existing safeguards to protect confidential customer information. My testimony today is intended to condemn the activities of pretexters and tell you about some of the ways we protect our customers' privacy while still rendering quick and convenient service to our customers. Providing additional protection for customer

information is not difficult: the difficult part is balancing protection and the customer's desire for convenience in a dynamic environment of technological and competitive change. The task is made more difficult by the ingenuity of those who would steal our customers' private information.

For example, hypothetically we could implement an eighteen - digit passcode requirement before customers could access their calling records. This act would make customer account information very secure --if anybody could remember and use it -- but I doubt anyone would. Therefore, this extremely secure passcode would not serve the interests of many, if any, of our 50 million plus wireless customers and millions more of our wireline customers. At Sprint Nextel we have sought to strike the proper balance between effective privacy protections and ease of access.

Sprint Nextel has been recognized for having first-in-class data security. In a June 2005 research report, the Aberdeen Group identified Sprint Nextel as the only telecommunications firm employing "Best Practice in Security for Governance in 2005." This award was based on Aberdeen Group's research involving 200 companies from various industries, known to be operating at best-in-class levels.

Sprint Nextel's day-to-day practices reflect our commitment to protecting the security of our customers' private account information. We understand that good information security cannot be achieved with any one safeguard, as human ingenuity is limitless. That is why we are vigilant on all fronts. For instance, we retain customer information necessary for us to communicate with and bill our customers behind a series of firewalls and other intrusion protection systems. Our certified information security

specialists constantly work to enhance our information protection system as technology evolves.

We work hard to address the human element: customer care representatives are there to serve the customer's desires, so our thousands of care representatives must constantly be on guard to distinguish genuine customer requests from efforts to steal information. We know from information obtained in litigation against data brokers that our efforts to train our customer care representatives to be on guard are effective. We require our employees and contractors to abide by a Code of Conduct that requires them to safeguard confidential customer information. We follow up by requiring them to take mandatory training on the protection of that information in accordance with the FCC's CPNI rules. This training is required of all employees, including senior management.

We publicize through our website how we collect, use and secure customer information, to whom we disclose that information, and why (http://www2.sprint.com/mr/consumertopic.do?topicId=680.). We regularly update our privacy policy and the consumer resources pointers on our website to answer frequently asked questions, address new issues, establish effective information protection practices, and advise customers how they can better protect their information. We do the same thing through other channels, such as bill inserts.

Our customer service agents are trained to ask for passcodes and follow detailed authentication procedures when responding to customer inquiries or requests relating to their accounts. It is important to keep in mind that most customers want fast and efficient customer service. That is their primary concern. Yet, customers often do not remember

their passcodes. Sprint Nextel's authentication procedures are designed to protect privacy while providing reasonably fast and efficient customer service.

When it comes to call detail records or other Customer Proprietary Network Information (CPNI), our company's policy, which goes beyond FCC requirements, is to allow access to the information only to those Sprint Nextel employees or agents with a "need to know." For example, customer service agents need to view this type of information in order to service accounts or answer billing questions. Customer service agents are trained to ask for a passcode during inbound calls. If a passcode has not been established or the customer does not remember the passcode, the agent must obtain customer specific information before answering questions about the customer's account.

We also contractually require our contractors and third party vendors to protect our customers' information, require them to take the same training our employees must take to protect customer privacy, and have threatened to terminate contracts for violation of those requirements.

We continually modify our systems in response to changes in the industry and technology. Given heightened recent concerns over privacy, we've made data security a priority in our merger integration process. In the process of combining our customer databases into a new, integrated billing platform, we're building new capabilities into that platform for authenticating persons who seek access to sensitive customer information. Not only will we employ password protection for all customers, we will ask customers who forget their passwords to use shared secrets like "who was your second grade teacher?" We will no longer employ private personal information that has become far too

easy to obtain as one fall-back method to authenticate their identity and allow access to their confidential information.

This is a massive undertaking that we will achieve through comprehensive systems. We believe that those capabilities will be the single most important step to better protect confidential customer information while still meeting our customers' need for efficiency and convenience. These changes, we believe, will give consumers the convenience they want while also providing the robust security they should have.

Sprint Nextel also encourages its customers to take specific precautions to protect their personal information from being accessed by others without their permission. For example, Sprint Nextel's website recommends that customers regularly change passwords used to access account information on the Sprint.com web site or when calling customer care, and to select unique passwords to access voicemail messages on Sprint Nextel phones.

Despite all of these protections and the deterrent effect they produce, pretexters still try to obtain information by pretending to be people they are not. They are skilled con artists who go to great lengths to obtain personal information on their targets in order to attempt to circumvent carrier protections. We should all be clear on this point: What pretexters are doing is wrong. They should be stopped and punished.

Our Corporate Security department has never found it necessary to engage in pretexting, nor has it ever engaged others to pretext on Sprint Nextel's behalf. We also do not believe that most pretexting is the result of dishonest employees. Our Office of Privacy has found that instances of such activity are extremely rare, and when they have occurred, the employees involved have been disciplined or fired.

In addition to system and employee efforts already mentioned, Sprint Nextel has devoted substantial resources to combat the pretexters. We have taken aggressive legal action against companies that we believe have fraudulently obtained, sold or distributed our customers' personal account information. Sprint Nextel filed lawsuits against three companies and an individual engaged in fraudulently obtaining and selling customer information and is actively considering additional lawsuits. The three lawsuits filed are:

- In January 2006, we sued 1st Source Information Specialists. This company engaged in the practice of pretexting for quite some time, and refused to stop selling Sprint Nextel customers' call detail records even after being sued by others. We ultimately obtained a permanent injunction against 1st Source, under which the company agreed to never again acquire, offer, sell or advertise the ability to obtain Sprint Nextel customer account information. Just last month, we reached a settlement with 1st Source and one of its principals. Although this settlement closes the case with respect to the corporate entity and one of its officers, the case continues against individual defendants who are also believed to be responsible for pretexting.
- Also in January 2006, we sued All Star Investigations, Inc. in Florida state court. Sprint Nextel quickly obtained a permanent injunction and reached a settlement with this company in June. Both parties are in the process of implementing this settlement now, and the defendant has turned over useful information concerning the pretexting business, information which we are using to improve our information security.

- In March 2006, Sprint Nextel sued San Marco & Associates, another Florida-based firm. This case is pending.

In addition to these lawsuits -- which have required us to expend substantial time and money- Sprint Nextel has sent scores of cease and desist letters to other entities who have advertised their ability to obtain call detail records or other private customer information. While we continue to identify companies engaged in pretexting, our experience is that the problem is less widespread today than it was one year ago even as reports of past pretexting continue to arise. Together with Congress, the Federal Trade Commission, the Federal Communications Commission, state Attorneys General, and the rest of the telecommunications industry, we have sent a message, loud and clear, that this fraudulent behavior will not be tolerated.

I appreciate the opportunity to appear before you today and share Sprint Nextel's perspective on its on-going efforts to protect customer privacy and its efforts to combat the pretexting problem. I would be happy to answer any questions.